UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF OHIO

RICHARD SLOVENKAY and **SARAH PHILLIPS,** on behalf of themselves and all others similarly situated, Plaintiffs, v. **LAKELAND COMMUNITY COLLEGE,** Defendant.	Case No. **JURY TRIAL DEMANDED**

CLASS ACTION COMPLAINT AND DEMAND FOR JURY TRIAL

Plaintiffs Richard Slovenkay and Sarah Phillips, individually and on behalf of all similarly situated persons, allege the following against Defendant, Lakeland Community College ("Lakeland"), based upon personal knowledge with respect to themselves and on information and belief derived from, among other things, investigation by their counsel and review of public documents as to all other matters:

I. INTRODUCTION

1. Plaintiffs bring this class action against Lakeland for its failure to properly secure and safeguard Plaintiffs' and other similarly situated individuals, including current and former students' and employees' names and Social Security numbers (the "Private Information") from cybercriminals.

2. Lakeland, based in Kirtland, Ohio, is a community college that serves (and has served) hundreds of thousands of students in their educational pursuits.

3. On or about September 19, 2023, Lakeland sent out data breach notice letters (the "Notice") to individuals whose information was compromised as a result of the incident.

4. Based on the Notice, Lakeland discovered that an unauthorized party had access to Plaintiffs' and Class Members' Private Information between March 7, 2023, and March 31, 2023 (the "Data Breach").

5. Plaintiffs and "Class Members" (defined below) were, and continue to be, at significant risk of identity theft and various other forms of personal, social, and financial harm. The risk will remain for their respective lifetimes.

6. Armed with the Private Information accessed in the Data Breach, data thieves can commit a variety of crimes including, *e.g.*, opening new financial accounts in Class Members' names, taking out loans in Class Members' names, using Class Members' information to obtain government benefits, and filing fraudulent tax returns using Class Members' information.

7. There has been no assurance offered by Lakeland that all personal data or copies of data have been recovered or destroyed, or that Defendant has adequately enhanced its data security practices sufficient to avoid a similar breach of its network in the future.

8. Therefore, Plaintiffs and Class Members have suffered and are at an imminent, immediate, and continuing increased risk of suffering ascertainable losses in the form of harm from identity theft and other fraudulent misuse of their Private Information, the loss of the benefit of their bargain, out-of-pocket expenses incurred to remedy or mitigate the effects of the Data Breach, and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach.

9. Plaintiffs bring this class action lawsuit to address Lakeland's inadequate safeguarding of Class Members' Private Information that it collected and maintained.

10. The potential for improper disclosure and theft of Plaintiffs' and Class Members' Private Information was a known risk to Lakeland, and thus Lakeland was on notice that failing to take necessary steps to secure the Private Information left it vulnerable to cyber-attacks.

11. Upon information and belief, Lakeland failed to properly monitor its systems and implement adequate data security practices with regard to the computer network and systems that housed Plaintiff's and Class Members' Private Information. Had Lakeland properly monitored its network, it could have prevented the Data Breach.

12. Plaintiffs' and Class Members' identities are now at risk as the Private Information that Lakeland collected and maintained is now in the hands of data thieves and other unauthorized third parties.

13. Plaintiffs seek to remedy these harms on behalf of themselves and all similarly situated individuals whose Private Information was accessed and compromised during the Data Breach.

14. Accordingly, Plaintiffs, on behalf of themselves and the Class, assert claims for breach of contract, breach of implied contract, and unjust enrichment.

II. PARTIES

15. Plaintiff Slovenkay is, and at all times mentioned herein was, an individual citizen of the State of Ohio.

16. Plaintiff Phillips is, and at all times mentioned herein was, an individual citizen of the State of Ohio.

17. Defendant Lakeland is a community college incorporated in Ohio with its principal place of business at 7700 Clocktower Drive, Kirtland, Ohio, 44094 in Lake County.

III. JURISDICTION AND VENUE

18. The Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5 million, exclusive of interest and costs. Upon information and belief, the number of Class Members is over 100, many of whom have different citizenship from Lakeland. Thus, minimal diversity exists under 28 U.S.C. § 1332(d)(2)(A).

19. This Court has jurisdiction over Lakeland because Lakeland operates in and/or is incorporated in this District.

20. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(a)(1) because a substantial part of the events giving rise to this action occurred in this District and Lakeland has harmed Class Members residing in this District.

IV. FACTUAL ALLEGATIONS

A. Lakeland's Business and Collection of Plaintiffs' and Class Members' Private Information

21. Lakeland is a community college located in Ohio serving its students both in-person and online. Founded in 1967, Lakeland offers various degree programs designed to prepare students to enter the workforce. Lakeland has served hundreds of thousands of students in their educational pursuits.

22. Lakeland currently employs 924 people and generates approximately $17.8 million in annual revenue.

23. Lakeland requires that its students and employees entrust it with highly sensitive personal information. Thus, in the ordinary course of receiving employment and educational services from Lakeland, Plaintiffs and Class Members were required to provide their Private Information to Defendant.

24. In its Privacy Assurance, Lakeland promises its students and employees that it would "protect the quality and integrity of your personally identifiable information."[1] Lakeland further informs all who entrust their Private Information to Lakeland that Lakeland is "committed to ethical business practices and compliance with all applicable laws, regulations, and policies that govern the privacy of Covered Data."[2]

25. Because of the highly sensitive and personal nature of the information Lakeland acquires and stores with respect to its students and employees, Lakeland also promises to, among other things, keep its students' and employees' Private Information private; comply with industry standards related to data security and the maintenance of its students' and employees' Private Information; inform its students and employees of its legal duties relating to data security and comply with all federal and state laws protecting students' and employees' Private Information; only use and release students' and employees' Private Information for reasons that relate to the services it provides; and provide adequate notice to students and employees if their Private Information is disclosed without authorization.

26. By obtaining, collecting, using, and deriving a benefit from Plaintiffs' and Class Members' Private Information, Lakeland assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiffs' and Class Members' Private Information from unauthorized disclosure and exfiltration.

27. Plaintiffs and Class Members relied on Lakeland to keep their Private Information confidential and securely maintained and to only make authorized disclosures of this information, which Defendant ultimately failed to do.

---

[1] *See* https://www.lakelandcc.edu/web/about/privacy-assurance (last visited Sept. 25, 2023).

[2] *See* https://www.lakelandcc.edu/web/public-policies-and-procedures/policies/3354-2-11-04 (last visited Sept. 25, 2023).

B. The Data Breach and Lakeland's Inadequate Notice to Plaintiffs and Class Members

28. According to Defendant's Notice, it discovered unauthorized access to its systems having taken place between March 7, 2023, and March 31, 2023, yet it took Lakeland until mid-September of 2023 to finally provide notice to Plaintiffs and Class Members of the compromise of their Private Information.

29. Through the Data Breach, the unauthorized cybercriminal(s) accessed a cache of highly sensitive Private Information, including full names in connection with Social Security numbers.

30. Lakeland had obligations created by contract, industry standards, common law, and representations made to Plaintiffs and Class Members to keep Plaintiffs' and Class Members' Private Information confidential and to protect it from unauthorized access and disclosure.

31. Plaintiffs and Class Members provided their Private Information to Lakeland with the reasonable expectation and mutual understanding that Lakeland would comply with its obligations to keep such information confidential and secure from unauthorized access and to provide timely notice of any security breaches.

32. Lakeland's data security obligations were particularly important given the substantial increase in cyberattacks in recent years.

33. Lakeland knew or should have known that its electronic records would be targeted by cybercriminals.

C. Lakeland Failed to Comply with FTC Guidelines

34. The Federal Trade Commission ("FTC") has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision

making. Indeed, the FTC has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. *See, e.g., FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015).

35. In October 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cybersecurity guidelines for businesses. The guidelines note that businesses should protect the personal customer information that they keep, properly dispose of personal information that is no longer needed, encrypt information stored on computer networks, understand their network's vulnerabilities, and implement policies to correct any security problems. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs, monitor all incoming traffic for activity indicating someone is attempting to hack into the system, watch for large amounts of data being transmitted from the system, and have a response plan ready in the event of a breach.

36. The FTC further recommends that companies not maintain personally identifiable information ("PII") longer than is needed for authorization of a transaction, limit access to sensitive data, require complex passwords to be used on networks, use industry-tested methods for security, monitor the network for suspicious activity, and verify that third-party service providers have implemented reasonable security measures.

37. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data by treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by the FTCA. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

38. As evidenced by the Data Breach, Lakeland failed to properly implement basic data security practices. Lakeland's failure to employ reasonable and appropriate measures to protect against unauthorized access to Plaintiffs' and Class Members' Private Information constitutes an unfair act or practice prohibited by Section 5 of the FTCA.

39. Lakeland was at all times fully aware of its obligation to protect the Private Information of its students and employees yet failed to comply with such obligations. Defendant was also aware of the significant repercussions that would result from its failure to do so.

D. Lakeland Failed to Comply with Industry Standards

40. As noted above, experts studying cybersecurity routinely identify businesses as being particularly vulnerable to cyberattacks because of the value of the Private Information which they collect and maintain.

41. Some industry best practices that should be implemented by businesses like Lakeland include but are not limited to: educating all employees, strong password requirements, multilayer security including firewalls, anti-virus and anti-malware software, encryption, multi-factor authentication, backing up data, and limiting which employees can access sensitive data. As evidenced by the Data Breach, Defendant failed to follow some or all of these industry best practices.

42. Other best cybersecurity practices that are standard in the industry include: installing appropriate malware detection software; monitoring and limiting network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches, and routers; monitoring and protecting physical security systems; and training staff regarding these points. As evidenced by the Data Breach, Defendant failed to follow these cybersecurity best practices.

43. Defendant failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

44. Defendant failed to comply with these accepted standards, thereby permitting the Data Breach to occur.

E. Lakeland Breached its Duty to Safeguard Plaintiffs' and Class Members' Private Information

45. In addition to its obligations under federal and state laws, Lakeland owed a duty to Plaintiffs and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the Private Information in its possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons. Lakeland owed a duty to Plaintiffs and Class Members to provide reasonable security, including complying with industry standards and requirements, training for its staff, and ensuring that its computer systems, networks, and protocols adequately protected the Private Information of Class Members

46. Lakeland breached its obligations to Plaintiffs and Class Members because it failed to properly maintain and safeguard its computer systems and data. Lakeland's unlawful conduct includes, but is not limited to, the following acts and/or omissions:

a. Failing to maintain an adequate data security system that would reduce the risk of data breaches and cyberattacks;

b. Failing to adequately protect student and employee Private Information;

c. Failing to properly monitor its own data security systems for existing intrusions;

d. Failing to sufficiently train its employees regarding the proper handling of its current and former students' and employees' Private Information;

e. Failing to fully comply with FTC guidelines for cybersecurity in violation of the FTCA;

f. Failing to adhere to industry standards for cybersecurity as discussed above; and

g. Otherwise breaching its duties and obligations to protect Plaintiffs' and Class Members' Private Information.

47. Lakeland unlawfully failed to safeguard Plaintiffs' and Class Members' Private Information by allowing cyberthieves to access its computer network and systems which contained unsecured and unencrypted Private Information.

48. Had Lakeland remedied the deficiencies in its information storage and security systems, followed industry guidelines, and adopted security measures recommended by experts in the field, it could have prevented intrusion into its information storage and security systems and, ultimately, the theft of Plaintiffs' and Class Members' confidential Private Information.

49. Accordingly, Plaintiffs' and Class Members' lives were severely disrupted. What's more, they have been harmed as a result of the Data Breach and now face an increased risk of future harm that includes, but is not limited to, fraud and identity theft. Plaintiffs and Class Members also lost the benefit of the bargain they made with Lakeland.

F. Lakeland Should Have Known that Cybercriminals Target Private Information to Carry Out Fraud and Identity Theft

50. The FTC hosted a workshop to discuss "informational injuries," which are injuries that consumers like Plaintiffs and Class Members suffer from privacy and security incidents such

as data breaches or unauthorized disclosure of data.[3] Exposure of highly sensitive personal information that a consumer wishes to keep private may cause harm to the consumer, such as the ability to obtain or keep employment. Consumers' loss of trust in e-commerce also deprives them of the benefits provided by the full range of goods and services available which can have negative impacts on daily life.

51. Any victim of a data breach is exposed to serious ramifications regardless of the nature of the data that was breached. Indeed, the reason why criminals steal information is to monetize it. They do this by selling the spoils of their cyberattacks on the black market to identity thieves who desire to extort and harass victims or to take over victims' identities in order to engage in illegal financial transactions under the victims' names.

52. Because a person's identity is akin to a puzzle, the more accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take on the victim's identity or to otherwise harass or track the victim. For example, armed with just a name and date of birth, a data thief can utilize a hacking technique referred to as "social engineering" to obtain even more information about a victim's identity, such as a person's login credentials or Social Security number. Social engineering is a form of hacking whereby a data thief uses previously acquired information to manipulate individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails.

53. In fact, as technology advances, computer programs may scan the Internet with a wider scope to create a mosaic of information that may be used to link compromised information to an individual in ways that were not previously possible. This is known as the "mosaic effect."

[3] *FTC Information Injury Workshop, BE and BCP Staff Perspective,* Federal Trade Commission, (October 2018), *available at* https://www.ftc.gov/system/files/documents/reports/ftc-informational-injury-workshop-be-bcp-staff-perspective/informational_injury_workshop_staff_report_-_oct_2018_0.pdf (last visited on Sept. 25, 2023).

Names and dates of birth, combined with contact information like telephone numbers and email addresses, are very valuable to hackers and identity thieves as it allows them to access users' other accounts.

54. Thus, even if certain information was not purportedly involved in the Data Breach, the unauthorized parties could use Plaintiffs' and Class Members' Private Information to access accounts, including, but not limited to, email accounts and financial accounts, to engage in a wide variety of fraudulent activity against Plaintiffs and Class Members.

55. For these reasons, the FTC recommends that identity theft victims take several time-consuming steps to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert on their account (and an extended fraud alert that lasts for 7 years if someone steals the victim's identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a freeze on their credit, and correcting their credit reports.[4] However, these steps do not guarantee protection from identity theft but can only mitigate identity theft's long-lasting negative impacts.

56. Identity thieves can also use stolen personal information such as Social Security numbers for a variety of crimes, including credit card fraud, phone or utilities fraud, bank fraud, to obtain a driver's license or official identification card in the victim's name but with the thief's picture, to obtain government benefits, or to file a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's Social Security number, rent a house in the victim's name, receive medical services in the victim's name, and even give the victim's personal information to police during an arrest resulting in an arrest warrant being issued in the victim's name.

[4] *See IdentityTheft.gov*, Federal Trade Commission, *available at* https://www.identitytheft.gov/Steps (last visited Sept. 25, 2023).

57. PII is data that can be used to detect a specific individual. PII is a valuable property right. Its value is axiomatic, considering the value of big data in corporate America and the consequences of cyber thefts (which include heavy prison sentences). Even this obvious risk-to-reward analysis illustrates beyond doubt that PII has considerable market value.

58. The U.S. Attorney General stated in 2020 that consumers' sensitive personal information commonly stolen in data breaches "has economic value."[5] The increase in cyberattacks, and attendant risk of future attacks, was widely known and completely foreseeable to the public and to anyone in Defendant's industry.

59. The PII of consumers remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, PII can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200.[6] Experian reports that a stolen credit or debit card number can sell for $5 to $110 on the dark web and that the "*fullz*" (a term criminals who steal credit card information use to refer to a complete set of information on a fraud victim) sold for $30 in 2017.[7]

60. Furthermore, even information such as names, email addresses and phone numbers, can have value to a hacker. Beyond things like spamming students and employees, or launching phishing attacks using their names and emails, hackers, *inter alia*, can combine this information

[5] *See Attorney General William P. Barr Announces Indictment of Four Members of China's Military for Hacking into Equifax*, U.S. Dep't of Justice, Feb. 10, 2020, available at https://www.justice.gov/opa/speech/attorney-general-william-p-barr-announces-indictment-fourmembers-china-s-military (last visited on Sept. 25, 2023).

[6] *Your personal data is for sale on the dark web. Here's how much it costs,* Digital Trends, Oct. 16, 2019, *available at*: https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/ (last visited on Sept. 25, 2023).

[7] *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec. 6, 2017, *available at*: https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last visited on Sept. 25, 2023).

with other hacked data to build a more complete picture of an individual. It is often this type of piecing together of a puzzle that allows hackers to successfully carry out phishing attacks or social engineering attacks. This is reflected in recent reports, which warn that "[e]mail addresses are extremely valuable to threat actors who use them as part of their threat campaigns to compromise accounts and send phishing emails."[8]

61. The Dark Web Price Index of 2022, published by PrivacyAffairs[9] shows how valuable just email addresses alone can be, even when not associated with a financial account:

Email Database Dumps	**Avg. Price USD (2022)**
10,000,000 USA email addresses	$120
600,000 New Zealand email addresses	$110
2,400,000 million Canada email addresses	$100

62. Beyond using email addresses for hacking, the sale of a batch of illegally obtained email addresses can lead to increased spam emails. If an email address is swamped with spam, that address may become cumbersome or impossible to use, making it less valuable to its owner.

63. Likewise, the value of PII is increasingly evident in our digital economy. Many companies, including Lakeland, collect PII for purposes of data analytics and marketing. These companies, collect it to better target students, and shares it with third parties for similar purposes.[10]

[8] *See* https://www.magicspam.com/blog/dark-web-price-index-the-cost-of-email-data/ (last visited on Sept. 25, 2023).

[9] *See* https://www.privacyaffairs.com/dark-web-price-index-2022/ (last visited on Sept. 25, 2023).

[10] *See* https://robinhood.com/us/en/support/articles/privacy-policy/ (last visited on Sept. 25, 2023).

64. One author has noted: "Due, in part, to the use of PII in marketing decisions, commentators are conceptualizing PII as a commodity. Individual data points have concrete value, which can be traded on what is becoming a burgeoning market for PII."[11]

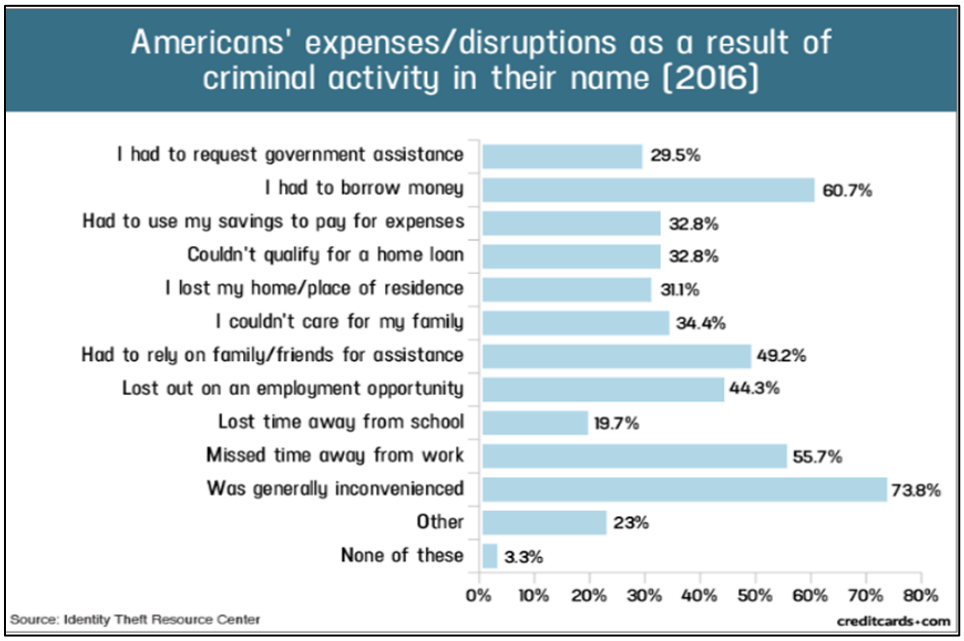
65. Consumers also recognize the value of their personal information and offer it in exchange for goods and services. The value of PII can be derived not only by a price at which consumers or hackers actually seek to sell it, but rather by the economic benefit consumers derive from being able to use it and control the use of it.

66. A consumer's ability to use their PII is encumbered when their identity or credit profile is infected by misuse or fraud. For example, a consumer with false or conflicting information on their credit report may be denied credit. Also, a consumer may be unable to open an electronic account where their email address is already associated with another user. In this sense, among others, the theft of PII in the Data Breach led to a diminution in value of the PII.

67. Data breaches, like that at issue here, damage consumers by interfering with their fiscal autonomy. Any past and potential future misuse of Plaintiffs' PII impairs their ability to participate in the economic marketplace.

[11] *See* John T. Soma, *Corporate Privacy Trend: The "Value" of Personally Identifiable Information ('PII') Equals the "Value" of Financial Assets,* 15 Rich. J. L. & Tech. 11, 14 (2009).

68. A study by the Identity Theft Resource Center[12] shows the multitude of harms caused by fraudulent use of PII:



69. It must also be noted that there may be a substantial time lag between when harm occurs and when it is discovered, and also between when PII and/or personal financial information is stolen and when it is used. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:[13]

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.

[12] Steele, Jason, *Credit Card and ID Theft Statistics*, CreditCards.com (October 23, 2017), *available at* https://www.creditcards.com/credit-card-news/credit-card-security-id-theft-fraud-statistics-1276/ (last visited Sept. 25, 2023).

[13] *Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown*, GAO (June 2007), *available at* https://www.gao.gov/assets/270/262904.html (last visited Sept. 25, 2023).

70. PII is such a valuable commodity to identity thieves that once the information has been compromised, criminals often trade the information on the "cyber black market" for years.

71. As a result, Plaintiffs and Class Members are at an increased risk of fraud and identity theft for many years into the future. Thus, Plaintiffs and Class Members have no choice but to vigilantly monitor their accounts for many years to come.

G. Plaintiffs' and Class Members' Damages

Plaintiff Slovenkay

72. When Plaintiff Slovenkay first became a professor at Lakeland in 2011, Lakeland required that he provide it with substantial amounts of their Private Information.

73. When Plaintiff Phillips first became a student at Lakeland, they required that she provide the same Private Information as part of the enrollment process.

74. On or about September 19, 2023, Plaintiffs each received a letter which told them that their Private Information had been impacted during the Data Breach. The notice letter informed them that the Private Information compromised included their full names and Social Security numbers.

75. The notice letter offered Plaintiffs only one year of credit monitoring services, which is not sufficient given that Plaintiffs will now experience a lifetime of increased risk of identity theft and other forms of targeted fraudulent misuse of their Private Information.

76. Plaintiffs and Class Members have been damaged by the compromise of their Private Information in the Data Breach.

77. Plaintiffs and Class Members entrusted their Private Information to Defendant in order to become students and employees and receive Defendant's academic services and employment offerings.

78. Plaintiffs' Private Information was subsequently compromised as a direct and proximate result of the Data Breach, which Data Breach resulted from Defendant's inadequate data security practices.

79. As a direct and proximate result of Lakeland's actions and omissions, Plaintiffs and Class Members have been harmed and are at an imminent, immediate, and continuing increased risk of harm, including but not limited to, having medical services billed in their names, loans opened in their names, tax returns filed in their names, utility bills opened in their names, credit card accounts opened in their names, and other forms of identity theft.

80. Further, as a direct and proximate result of Lakeland's conduct, Plaintiffs and Class Members have been forced to expend time dealing with the effects of the Data Breach and have incurred costs associated with time spent and the loss of productivity from taking time to address and attempting to ameliorate, mitigate, and deal with the actual and future consequences of the Data Breach.

81. Plaintiffs and Class Members also face a substantial risk of being targeted in future phishing, data intrusion, and other illegal schemes through the misuse of their Private Information, since potential fraudsters will likely use such Private Information to carry out such targeted schemes against Plaintiffs and Class Members.

82. Additionally, Plaintiffs and Class Members have experienced the stress, nuisance and annoyance of dealing with all issues resulting from the Data Breach.

83. The Private Information maintained by and stolen from Defendant's systems, combined with publicly available information, allows nefarious actors to assemble a detailed mosaic of Plaintiffs and Class Members, which can also be used to carry out targeted fraudulent schemes against Plaintiffs and Class Members.

84. Plaintiffs and Class Members also lost the benefit of the bargain they made with Lakeland. Plaintiffs and Class Members overpaid for academic services that were intended to be accompanied by adequate data security but were not. Indeed, part of the price Plaintiffs and Class Members paid to Lakeland was intended to be used by Lakeland to fund adequate security of Lakeland's system and protect Plaintiffs' and Class Members' Private Information. Thus, Plaintiffs and the Class did not receive what they paid for.

85. Additionally, Plaintiffs and Class Members have experienced damages to and diminution in value of their Private Information entrusted to Lakeland for the sole purpose of obtaining an education from Lakeland, with the mutual understanding that Lakeland would safeguard Plaintiffs' and Class Members' Private Information against theft and not allow access to and misuse of their Information by others.

86. Finally, Plaintiffs and Class Members have suffered or will suffer actual injury as a direct and proximate result of the Data Breach in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach.

87. Moreover, Plaintiffs and Class Members have an interest in ensuring that their Private Information, which is believed to still be in the possession of Lakeland, is protected from future additional breaches by the implementation of more adequate data security measures and safeguards, including but not limited to, ensuring that the storage of data or documents containing personal and financial information is not accessible online, that access to such data is password-protected, and that such data is properly encrypted.

88. As a direct and proximate result of Lakeland's actions and inactions, Plaintiffs and Class Members have suffered a loss of privacy and have suffered cognizable harm, including an imminent and substantial future risk of harm, in the forms set forth above.

V. CLASS ACTION ALLEGATIONS

89. Plaintiffs bring this action individually and on behalf of all other persons similarly situated, pursuant to Federal Rule of Civil Procedure 23(a), 23(b)(1), 23(b)(2), and 23(b)(3).

90. Specifically, Plaintiffs propose the following Nationwide Class (also referred to herein as the "Class") subject to amendment as appropriate:

> All individuals who had Private Information accessed and/or acquired as a result of the Data Breach, including all current and former students and employees who were sent a notice of the Data Breach.

91. Excluded from the Class are Defendant and its parents or subsidiaries, any entities in which it has a controlling interest, as well as its officers, directors, affiliates, legal representatives, heirs, predecessors, successors, and assigns. Also excluded is any Judge to whom this case is assigned as well as their judicial staff and immediate family members.

92. Plaintiffs reserve the right to modify or amend the definition of the proposed Class or add subclasses before the Court determines whether certification is appropriate.

93. The proposed Class meets the criteria for certification under Fed. R. Civ. P. 23(a), (b)(2), and (b)(3).

94. Numerosity. The Class Members are so numerous that joinder of all members is impracticable. Though the exact number and identities of Class Members are unknown at this time, based on information and belief, the Class consists of over 285,000 current and former students and employees of Lakeland whose data was compromised in the Data Breach. The identities of Class Members are ascertainable through Lakeland's records, Class Members' records, publication notice, self-identification, and other means.

95. Commonality. There are questions of law and fact common to the Class which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

a. Whether Lakeland engaged in the conduct alleged herein;

b. When Lakeland learned of the Data Breach;

c. Whether Lakeland's response to the Data Breach was adequate;

d. Whether Lakeland unlawfully lost or disclosed Plaintiffs' and Class Members' Private Information;

e. Whether Lakeland failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the Private Information compromised in the Data Breach;

f. Whether Lakeland's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;

g. Whether Lakeland's data security systems prior to and during the Data Breach were consistent with industry standards;

h. Whether Lakeland owed a duty to Class Members to safeguard their Private Information;

i. Whether Lakeland breached its duty to Class Members to safeguard their Private Information;

j. Whether hackers obtained Class Members' Private Information via the Data Breach;

k. Whether Lakeland had a legal duty to provide timely and accurate notice of the Data Breach to Plaintiffs and the Class Members;

l. Whether Lakeland breached its duty to provide timely and accurate notice of the Data Breach to Plaintiffs and Class Members;

m. Whether Lakeland knew or should have known that its data security systems and monitoring processes were deficient;

n. What damages Plaintiffs and Class Members suffered as a result of Lakeland's misconduct;

o. Whether Lakeland was unjustly enriched;

p. Whether Plaintiffs and Class Members are entitled to actual and/or statutory damages;

q. Whether Plaintiffs and Class Members are entitled to additional credit or identity monitoring and monetary relief; and

r. Whether Plaintiffs and Class Members are entitled to equitable relief, including injunctive relief, restitution, disgorgement, and/or the establishment of a constructive trust.

96. Typicality. Plaintiffs' claims are typical of those of other Class Members because Plaintiffs' Private Information, like that of every other Class Member, was compromised in the Data Breach.

97. Adequacy of Representation. Plaintiffs will fairly and adequately represent and protect the interests of Class Members. Plaintiffs' counsel is competent and experienced in litigating class actions, including data privacy litigation of this kind.

98. Predominance. Lakeland has engaged in a common course of conduct toward Plaintiffs and Class Members in that all of Plaintiffs' and Class Members' data was stored on the same computer systems and unlawfully accessed and exfiltrated in the same way. The common

issues arising from Lakeland's conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

99. Superiority. A class action is superior to other available methods for the fair and efficient adjudication of this controversy and no unusual difficulties are likely to be encountered in the management of this class action. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a Class action, most Class Members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for Lakeland. In contrast, conducting this action as a class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class Member.

100. Class certification is also appropriate under Fed. R. Civ. P. 23(b)(2). Lakeland has acted and/or refused to act on grounds generally applicable to the Class such that final injunctive relief and/or corresponding declaratory relief is appropriate as to the Class as a whole.

101. Finally, all members of the proposed Class are readily ascertainable. Lakeland has access to the names and addresses and/or email addresses of Class Members affected by the Data Breach. Class Members have already been preliminarily identified and sent notice of the Data Breach by Lakeland.

VI. CLAIMS FOR RELIEF

COUNT I
BREACH OF CONTRACT
(On behalf of Plaintiffs and the Class)

102. Plaintiffs restate and reallege the allegations in the foregoing paragraphs as if fully set forth herein.

103. Plaintiffs and Class Members entered into a valid and enforceable contract through which they paid money to Lakeland in exchange for educational and other services. That contract included promises by Defendant to secure, safeguard, and not disclose Plaintiffs' and Class Members' Private Information.

104. Lakeland's Privacy Policy memorialized the rights and obligations of Lakeland and its students and employees. This document was provided to Plaintiffs and Class Members in a manner in which it became part of the agreement for services.

105. In its Privacy Policy, Lakeland commits to protecting the privacy and security of the Private Information belonging to its students and employees, including Plaintiffs and Class Members, and promises to never share this Private Information except under certain limited circumstances.

106. Plaintiffs and Class Members fully performed their obligations under their contracts with Lakeland.

107. However, Lakeland did not secure, safeguard, and/or keep private Plaintiffs' and Class Members' Private Information, and therefore Lakeland breached its contracts with Plaintiffs and Class Members.

108. Lakeland allowed third parties to access, copy, and/or exfiltrate Plaintiffs' and Class Members' Private Information without permission. Therefore, Lakeland breached the Privacy Policy with Plaintiffs and Class Members.

109. Lakeland's failure to satisfy its confidentiality and privacy obligations resulted in Lakeland providing services to Plaintiffs and Class Members that were of a diminished value.

110. As a result, Plaintiffs and Class Members have been harmed, damaged, and/or injured as described herein, including in Defendant's failure to fully perform its part of the bargain with Plaintiffs and Class Members.

111. As a direct and proximate result of Lakeland's conduct, Plaintiffs and Class Members suffered and will continue to suffer damages in an amount to be proven at trial.

112. In addition to monetary relief, Plaintiffs and Class Members are also entitled to injunctive relief requiring Lakeland to, *inter alia*, strengthen its data security systems and monitoring procedures, conduct periodic audits of those systems, and provide lifetime credit monitoring and identity theft insurance to Plaintiffs and Class Members.

COUNT II
BREACH OF IMPLIED CONTRACT
(On behalf of Plaintiffs and the Class)

113. Plaintiffs restate and reallege the allegations in the foregoing paragraphs as if fully set forth herein.

114. This Count is pleaded in the alternative to Count I above.

115. Lakeland provided employment and academic services to Plaintiffs and Class Members. Plaintiffs and Class Members formed an implied contract with Defendant regarding the provision of those services through their collective conduct, including by Plaintiffs and Class Members paying for services from Defendant.

116. By providing employment and academic services, it knew or should have known that it must protect Plaintiffs' and Class Members' confidential Private Information in accordance with Lakeland's policies, practices, and applicable law.

117. As consideration, Plaintiffs and Class Members paid money to Lakeland and/or turned over valuable Private Information to Lakeland. Accordingly, Plaintiffs and Class Members bargained with Lakeland to securely maintain and store their Private Information.

118. Lakeland accepted possession of Plaintiffs' and Class Members' Private Information for the purpose of providing services to them.

119. In delivering their Private Information to Lakeland and/or paying for services, Plaintiffs and Class Members intended and understood that Lakeland would adequately safeguard the Private Information as part of that service.

120. Defendant's implied promises to Plaintiffs and Class Members include, but are not limited to, (1) taking steps to ensure that anyone who is granted access to Private Information also protect the confidentiality of that data; (2) taking steps to ensure that the Private Information that is placed in the control of its employees is restricted and limited to achieve an authorized business purpose; (3) restricting access to qualified and trained employees and/or agents; (4) designing and implementing appropriate retention policies to protect the Private Information against criminal data breaches; (5) applying or requiring proper encryption; (6) implementing multifactor authentication for access; and (7) taking other steps to protect against foreseeable data breaches.

121. Plaintiffs and Class Members would not have entrusted their Private Information to Lakeland in the absence of such an implied contract.

122. Had Lakeland disclosed to Plaintiffs and the Class that they did not have adequate computer systems and security practices to secure sensitive data, Plaintiffs and Class Members would not have provided their Private Information to Lakeland.

123. Lakeland recognized that Plaintiffs' and Class Member's Private Information is highly sensitive and must be protected, and that this protection was of material importance as part of the bargain to Plaintiffs and the other Class Members.

124. Lakeland violated these implied contracts by failing to employ reasonable and adequate security measures to secure Plaintiffs' and Class Members' Private Information.

125. Plaintiffs and Class Members have been damaged by Lakeland's conduct, including the harms and injuries arising from the Data Breach now and in the future, as alleged herein.

COUNT III
UNJUST ENRICHMENT
(On behalf of Plaintiffs and the Class)

126. Plaintiffs restate and reallege the allegations in the foregoing paragraphs as if fully set forth herein.

127. This Count is pleaded in the alternative to Counts I and II above.

128. Plaintiffs and Class Members conferred a benefit on Lakeland by turning over their Private Information to Defendant and/or by paying for services that should have included cybersecurity protection to protect their Private Information. Plaintiffs and Class Members did not receive such protection.

129. Upon information and belief, Lakeland funds its data security measures entirely from its general revenue, including from payments made to it by Plaintiffs and Class Members.

130. As such, a portion of the payments made by Plaintiffs and Class Members is to be used to provide a reasonable and adequate level of data security that is in compliance with applicable state and federal regulations and industry standards, and the amount of the portion of each payment made that is allocated to data security is known to Lakeland.

131. Lakeland has retained the benefits of its unlawful conduct, including the amounts of payment received from Plaintiffs and Class Members that should have been used for adequate cybersecurity practices that it failed to provide.

132. Lakeland knew that Plaintiffs and Class Members conferred a benefit upon it, which Lakeland accepted. Lakeland profited from these transactions and used the Private Information of Plaintiffs and Class Members for business purposes, while failing to use the payments it received for adequate data security measures that would have secured Plaintiffs' and Class Members' Private Information and prevented the Data Breach.

133. If Plaintiffs and Class Members had known that Lakeland had not adequately secured their Private Information, they would not have agreed to provide such Private Information to Defendant.

134. Due to Lakeland's conduct alleged herein, it would be unjust and inequitable under the circumstances for Lakeland to be permitted to retain the benefit of its wrongful conduct.

135. As a direct and proximate result of Lakeland's conduct, Plaintiffs and Class Members have suffered and/or will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity to control how their Private Information is used; (iii) the compromise, publication, and/or theft of their Private Information; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their Private Information; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (vi) the continued risk to their Private Information, which remains in Lakeland's possession and is subject to further unauthorized disclosures so long as

Lakeland fails to undertake appropriate and adequate measures to protect Private Information in its continued possession; and (vii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the Private Information compromised as a result of the Data Breach for the remainder of the lives of Plaintiffs and Class Members.

136. Plaintiffs and Class Members are entitled to full refunds, restitution, and/or damages from Lakeland and/or an order proportionally disgorging all profits, benefits, and other compensation obtained by Lakeland from its wrongful conduct. This can be accomplished by establishing a constructive trust from which the Plaintiffs and Class Members may seek restitution or compensation.

137. Plaintiffs and Class Members may not have an adequate remedy at law against Lakeland, and accordingly, they plead this claim for unjust enrichment in addition to, or in the alternative to, other claims pleaded herein.

VII. PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, on behalf of themselves and the Class described above, seek the following relief:

a. An order certifying this action as a Class action under Fed. R. Civ. P. 23, defining the Class as requested herein, appointing the undersigned as Class counsel, and finding that Plaintiffs are proper representatives of the Class requested herein;

b. Judgment in favor of Plaintiffs and Class Members awarding them appropriate monetary relief, including actual damages, statutory damages, equitable relief, restitution, disgorgement, and statutory costs;

c. An order providing injunctive and other equitable relief as necessary to protect the interests of the Class, including but not limited to an order:

1. prohibiting Defendant from engaging in the wrongful and unlawful acts described herein;
2. requiring Defendant to protect, including through encryption, all data collected through the course of their business in accordance with all applicable regulations, industry standards, and federal, state or local laws;
3. requiring Defendant to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the PII of Plaintiff and Class Members;
4. prohibiting Defendant from maintaining the PII of Plaintiffs and Class Members on a cloud-based database;
5. requiring Defendant to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;
6. requiring Defendant to engage independent third-party security auditors and internal personnel to run automated security monitoring;
7. requiring Defendant to audit, test, and train their security personnel regarding any new or modified procedures;
8. requiring Defendant to segment data by, among other things, creating firewalls and access controls so that if one area of Defendant's network is compromised, hackers cannot gain access to other portions of Defendant's

systems;

9. requiring Defendant to conduct regular database scanning and securing checks;
10. requiring Defendant to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling personal identifying information, as well as protecting the personal identifying information of Plaintiffs and Class Members;
11. requiring Defendant to routinely and continually conduct internal training and education, and on an annual basis to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;
12. requiring Defendant to implement a system of tests to assess its respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with Defendant's policies, programs, and systems for protecting personal identifying information;
13. requiring Defendant to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor its information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;
14. requiring Defendant to meaningfully educate all Class Members about the

threats that they face as a result of the loss of their confidential personal identifying information to third parties, as well as the steps affected individuals must take to protect themselves; and

15. requiring Defendant to implement logging and monitoring programs sufficient to track traffic to and from Defendant's servers; and for a period of 10 years, appointing a qualified and independent third party assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate Defendant's compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the class, and to report any deficiencies with compliance of the Court's final judgment;

d. An order instructing Lakeland to purchase or provide funds for lifetime credit monitoring and identity theft insurance to Plaintiffs and Class Members;

e. An order requiring Lakeland to pay the costs involved in notifying Class Members about the judgment and administering the claims process;

f. A judgment in favor of Plaintiffs and Class Members awarding them prejudgment and post-judgment interest, reasonable attorneys' fees, costs, and expenses as allowable by law; and

g. An award of such other and further relief as this Court may deem just and proper.

VIII. DEMAND FOR JURY TRIAL

Plaintiffs demand a trial by jury on all triable issues.

DATED: September 26, 2023.

Respectfully submitted,

/s/Christopher Wiest
Christopher Wiest (Ohio 0077931)
25 Town Center Blvd., Suite 104
Crestview, KY 41017
Tel: (513) 257-1895
Fax: (859) 495-0803
chris@cwiestlaw.com

Mason A. Barney*
Tyler J. Bean*
SIRI & GLIMSTAD LLP
745 Fifth Avenue, Suite 500
New York, New York 10151
Tel: (212) 532-1091
mbarney@sirillp.com
tbean@sirillp.com

**pro hac vice applications to be filed*

Attorneys for Plaintiffs and the Putative Class